C.6.1.6 PERSONNEL AND PHYSICAL SECURITY

C.6.1.6.1 MANDATORY REQUIREMENTS

1) Within the accreditation boundary, ETS2 shall meet or exceed the following mandatory requirements for personnel and physical security. See Attachment 4*, Background Investigation Process for ETS2 Contractors and Their Subcontractors*, for clarification of the required background investigation level. The Contractor shall restrict personnel access to ETS2 to those with a need to know;

2) Based on the Privacy Act and GSA Order CIO P 2181.1–HSPD-12, “Personal Identity Verification and Credentialing Handbook,” the physical site where the hardware resides shall be secured as a General Support System in accordance with NIST 800-18-Rev.1 (or latest), “Guide for Developing Security Plans for Federal Information Technology Systems,” and the CIO P 2100.1F, “GSA Information Technology (IT) Security Policy,” and shall be staffed by an appropriate mix of National Agency Check with Inquiries (NACI or equivalent Tier 1) and Moderate Risk Background Investigation (MBI or equivalent Tier 2S) investigations for staff and supervisory personnel. The guidelines for the levels are based on HSPD-12 and GSA background check requirements. Unless otherwise directed, GSA shall assume responsibility for the cost of Contractor personnel background checks, including subcontractor(s)/teaming partner(s). At GSA’s discretion, the contractor may be required to resume payment for background checks as directed by GSA. If so, the Government shall provide written notification to the Contractor at least fourteen (14) calendar days in advance and the contractor shall resume payment for the contractor personnel background checks and subcontractor(s) teaming partners. The background checks shall follow GSA procedures and the Contractor shall submit the package through the ETS2 PMO as directed;

3) The Contractor shall assure that employees performing under this contract receive annual IT security training in accordance with OMB Circular A-130, “Management of Federal Information Resources”; the Federal Information Security Management Act of 2002 (FISMA); and NIST Special Publications 800-53 Rev. 3, “Recommended Security Controls for Federal Information Systems and Organizations” and 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems” requirements, with a specific emphasis on role based requirements and rules of behavior;

4) The Contractor shall record the security awareness training for each individual (name, date, successful completion or not) and provide to the ETS2 PMO on an annual basis or whenever is required on an ad hoc basis;

5) The Contractor’s ISSO/security manager shall within 48 hours notify the ETS2 PMO ISSO in writing when personnel having access to ETS2 changes either through termination both favorable and unfavorable or the addition of new staff;

6) The Contractor shall assure that access to ETS2 shall be granted to only those individuals and subcontractor(s)/teaming partner(s), including ETMCs, receiving a favorable adjudication of the HSPD-12 background investigation;

7) The Contractor shall contact the ETS2 PMO for approval of any non-U.S. citizens who are proposed to work as a contractor on ETS2 and are eligible for a HSPD-12 background investigation;

8) ETS2 shall by default provide privileged user accounts on a role-related, need-to-know basis. ETS2 shall restrict personnel access to those with a need-to-know in strict accordance with their roles and permissions, such as program/project manager, helpdesk, developer, administrator (engineer). Information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment will be limited;

9) Security roles shall be supervised by the ISSO and shall be separate personnel without other role (e.g. System, Network, Helpdesk, etc) in accordance with the concept of Separation of Duties; and

10) The ETS2 Contractor shall track, monitor and report privileged role assignments. Privileged user accounts will be reviewed and reevaluated annually. All privileged users will subscribe to security alerts, advisories, and directives to ensure up to date knowledge of requirements and changing security environment.

C.6.1.6.2 OBJECTIVES

ETS2 should, to the maximum extent possible, meet or exceed the following objective for personnel and physical security.

The Contractor should accommodate customer agency-specific personnel security requirements as ordered and specified by task order, including but not limited to ensuring that all contractor personnel meet applicable agency security and/or clearance requirements. The Contractor may propose staff with other security clearances provided their clearances meet or exceed the levels stated herein.